Exhibit 1

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

BRIAN HUDDLESTON, Plaintiff, vs. **FEDERAL BUREAU OF INVESTIGATION and UNITED STATES DEPARTMENT OF JUSTICE** Defendant	**Case No. 4:20-cv-447-ALM**

DECLARATION OF YAACOV APELBAUM

My name is Yaacov Apelbaum, I am greater than 18 years of age and competent to testify, and I do testify as follows under penalty of perjury under the laws of the United States, as witnessed by my signature below:

(1) I previously submitted a copy of my curriculum vitae (Dkt. #141-3), and I attest that its contents are true and correct.

(2) I serve as a cyber intelligence and cyber forensic expert and consultant to Mr. Huddleston via his counsel, Ty Clevenger.

(3) In his declaration, Shannon R. Hammer testifies as follows:

> In addition to the types of records listed in the FBI's Vaughn index, there are potentially thousands of files on the Work laptop that cannot be viewed or processed pursuant to the FOIA. These file types include operating system files (e.g., .exe files), Resilient File System (ReFS), New Technology File System (NTFS), and File Allocation Table (FAT).

Declaration of Shannon R. Hammer (Dkt. 196-1) ¶7. In my professional opinion, Mr. Hammer's testimony is technically inaccurate. All of the foregoing files can be reviewed using readily available tools, and this is widely known in the information technology and digital forensic fields. In fact, this basic knowledge is publicly accessible, even through simple web searches. For example, the following are industry-standard tools for FAT File Analysis and Recovery:

A. The Sleuth Kit (TSK) & Autopsy
- *Status*: Industry standard in law enforcement, corporate forensics, and academia
- *Use*: Full file system analysis, including FAT12, FAT16, and FAT32. Allows detailed examination of metadata, deleted file recovery, and timeline creation
- *Why it's standard*: Court-admissible, well-documented, supports scripting and batch processing

B. EnCase Forensic (by OpenText)
- *Status*: Gold standard in enterprise and legal forensics
- *Use*: Full disk imaging, FAT file parsing, hash matching, and legal chain-of-custody tracking
- *Why it's standard*: Widely accepted in courts, used by government and private forensic investigators

C. FTK (Forensic Toolkit by Exterro)
- *Status*: Top-tier enterprise tool
- *Use*: Data carving, FAT volume recovery, memory analysis
- *Why it's standard*: Built-in file parsing modules, keyword indexing, and chain-of-custody support

D. X-Ways Forensics
- *Status*: Preferred by experts for low-level analysis
- *Use*: Sector-level analysis of FAT structures, efficient for parsing boot sectors, directory entries, and MFT
- *Why it's standard*: Lightweight, fast, highly detailed forensic data views

E. R-Studio
- *Status*: Commercial recovery tool used in both forensics and IT departments
- *Use*: Recovery from FAT32, exFAT partitions—especially useful in data loss from USB, SD cards, etc.

F. Hex Editors and Low-Level Inspectors
- *Tools*: WinHex, HxD, 010 Editor
- *Use*: Manual inspection of FAT table entries, boot sectors, and directory records
- *Why it's standard*: Essential for deep-dive forensic cases and reverse engineering

(4) It appears that Asst. U.S. Attorney Michael P. Spence also has provided a statement that is technically inaccurate. Paragraph 5 of his declaration (Dkt. #196-2) is identical to Paragraph 7 of Mr. Hammer's declaration. Given that the same language appears in both declarations, it raises questions as to whether a full technical review was performed prior to submission. I defer to the Court regarding any legal conclusions.

(5) I used FAT files as an example because they are particularly important to this case. I have attached the declaration and CV of William Binney, the former technical director of the National Security Agency, as Exhibits A and B to my declaration. I have also attached the declaration and CV of computer forensics expert witness Peter Clay as Exhibits C and D to my declaration. Exhibits A-D were filed on May 9, 2019 in *U.S.A. v. Roger J. Stone, Jr.*, Case No. 1:19-cr-00018-ABJ (D.D.C.). As you can see from those declarations, Mr. Binney and Mr. Clay testified that the Democratic National Committee ("DNC") emails published by Wikileaks in 2016 appeared to have been downloaded onto a thumb drive rather than "hacked" remotely by Russian agents. In footnote 5 of their respective

declarations, Mr. Hammer and Mr. Pence correctly note that FAT files are affiliated with the metadata on flash drives, and "flash drive" is another term for "thumb drive." The FAT files are, therefore, critical records that would indicate whether the DNC emails were downloaded from Seth Rich's laptop to a thumb drive and then transferred to Wikileaks rather than being "hacked" remotely by Russian agents.

(6) In addition to the technical concerns described above, any credible forensic examination of digital media should follow standard procedures to ensure evidentiary integrity. These include:

- Creating a forensic image (bit-for-bit copy) of the original drive prior to analysis
- Accessing the image through a write blocker to prevent modification of original data
- Maintaining a complete, timestamped log of all actions taken during acquisition, processing, and review

To assess the quality and scope of work performed by the FBI, it is essential to verify whether these procedures were followed. Therefore, a detailed log of all steps taken during the review of the laptops must be produced, including the tools used, personnel involved, imaging records, hash verifications, and chain-of-custody documentation. Without such verification, the completeness and integrity of the analysis cannot be independently confirmed.

(7) The Vaughn indexes provided by the FBI fail to account for large volumes of metadata, including some of the most obvious, *e.g.,* the total number of gigabytes stored on the laptops and the total number of files. It appears that the FBI cherry-picked certain metadata about certain files but omitted the vast majority of metadata from the Vaughn indexes. If the FBI had provided the basics, e.g., the total gigabytes and number of files, then we could better estimate how much metadata is missing.

(8) The declarations of Mr. Hammer and Mr. Spence give no indication of the software tools utilized, the level of effort expended (*e.g.*, personnel hours), or the level of expertise of the personnel who performed the reviews of the electronic devices (*e.g.*, a skilled expert versus someone with limited experience). In light of the evidence set forth in my previous declaration (Dkt. #190) and the evidence set forth above, it is my professional opinion that neither the FBI nor the U.S. Attorney's Office for the District of Columbia made a diligent attempt to retrieve and review the files or the metadata from the electronic devices that belonged to Seth Rich.

THE DECLARANT SAYS NOTHING FURTHER.

May 9, 2025

Yaacov Apelbaum

Exhibit 1

Internal Exhibit A

William E. Binney

- Mathematician/Analyst -

Skill Areas: Intelligence Analysis; Traffic Analysis; Systems Analysis; Mathematics; Knowledge Management
Description of Most Recent Position

November 2005 - 30 June 2006 Entegra Systems Inc.
For the U.S. Customs and Border Protection, Office of Information Technology, Targeting and Analysis Systems Program Office, Mr. Binney defined statistical modeling techniques and advanced analytic processes, to support the modernization of CBP's Targeting and Analysis systems, tools, and analytical processes to perform predictive analysis of terror-related cargo and passenger transactions. Mr. Binney also supported the evaluation and integration of advanced analytic tools, both COTS tools and tools being develop by research universities and National Labs, under grants from the Department of Homeland Security, Advanced Research Projects Agency (HS/ARPA). Furthermore, Mr. Binney conducted an evaluation of CBP data quality, as well as defining techniques and processes for aggregating Cargo, Passenger, Law Enforcement, and Counter Terrorism-related data from multiple sources into a single, normalized entity-based repository.
Finally, Mr. Binney served as a member of a quick-reaction analytic team, which reviews available intelligence or information, and applies emerging advanced analytic technologies against selected operational data sets, to support executive level decision making and field operations.

Past Positions
From 2002 to 2004, as a member of Entity Mapping LLC., I worked on a contract for a major government organization. The contract effort centered on analysis of data to produce new entities and communities of interest. This effort required development of new data management processes, as well as analytic techniques to first verify the relationships between known entities of interest, then predict the existence of other entities of interest not previously observed. Our efforts also resulted in successfully developing a rules-based exclusionary approach that resulted in automatic discovery of newly observed but unpredicted entities of interest.

Positions held during 32 years career at the National Security Agency

2001	Technical Leader, Intelligence
1999-2001	Representative to the National Technology Alliance Executive Board
1996-2001	Member of the Senior Technical Review Panel
1995-2001	Co-founder/leader of the Automation Research Center (ARC)
2000-2001	Technical Director of the Analytic Services Office
1998-2000	Chair of the Technical Advisory Panel to the Foreign Relations Council
1998-2000	Analysis Skill Field Leader, Operations
1997-2000	Technical Director, World Geopolitical and Military
1996-1997	Technical Director, Russia
1975-1996	Leading analyst for warning, Russia

EXHIBIT
tabbies
1

1970-1975 Analyst on Russia
Military service
1965-1969 Four years in the Army Security Agency (NSAICSS)

Career Experience:
Over the years, I, have applied mathematical, discipline to collection, analysis and reporting. In the process, I formulated Set Theory, Number Theory and Probability applications to collection, data analysis and intelligence analysis. Based on this experience, I was able to structure analysis, and transform it into a definable discipline making it possible to code and automatically execute these functions without human intervention from the point of collection to the end report. The successful automation of analysis formed the foundation for prototype developments in the ARC. These efforts caught the eye of Congressional Staffers and captured their imaginations. So much so that Congress actively supported and funded ARC development of automated systems. These systems revolutionized the business processes by demonstrating how to handle massive amounts of data effectively and relate results to military and other customers. I have also organized an international coalition of countries to jointly develop technology,. share results and gain the benefits of collaborative efforts. Primarily, I have focused on solving problems from a systems analysis perspective so that gains in any part of the business could be leveraged across the entire business enterprise.

Honors, awards and special achievements:
Directors Productivity Award - 1995
Technical Achievement Award - 1998
Gold Nugget Award - 1988
Numerous Letters of Appreciation Numerous cash awards

Degrees and Certificates:
B. S. Mathematics, The Pennsylvania State University, 1970 Certified Analysis Professional - 1973

Exhibit 1

Internal Exhibit B

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA

v.

No. 19-cr-18 (ABJ)

ROGER J. STONE, JR.

Defendant.

______________________________/

DECLARATION OF WILLIAM E. BINNEY

I am William Binney and I hereby declare:

Background

1. I am a Cryptanalyst-mathematician.

2. I am a former employee of the National Security Agency ("NSA").

3. I was a Russia specialist and worked in the operations side of intelligence, starting as an analyst and ending as a Technical Director prior to becoming a geopolitical world Technical Director.

4. Between 1965 and 1969, I spent four years working in the U.S. Army Security Agency (the "ASA"). Until 1976, the ASA was the signals intelligence operation for the U.S. Army. Its mission was to intercept, acquire and decipher communications between persons, in electronic or any other form.

5. A true and correct copy of my resume is attached hereto as Exhibit 1.

6. After the Army, I spent 32 years working at the National Security Agency (the "NSA"). The NSA is the signals intelligence agency within the Department of Defense.

7. At the NSA, I held a variety of positions.
These included the following positions:

2001 - Technical Leader, Intelligence

1999-2001 - Representative to the National Technology Alliance Executive Board
1996-2001 - Member of the Senior Technical Review Panel
1995-2001 - Co-founder/leader of the Automation Research Center (ARC
2000-2001 - Technical Director of the Analytic Services Office
1998-2000 - Chair of the Technical Advisory Panel to the Foreign Relation Council
1998-2000 - Analysis Skill Field Leader, Operations
1997-2000 - Technical Director, World Geopolitical and Military
1996-1997 - Technical Director, Russia
1975-1996 - Leading analyst for warning, Russia
1970-1975 - Analyst on Russia

9. When I left the NSA in 2001, I was the Technical Leader for intelligence at the agency. As Technical Leader, I was the senior technical person in analysis at the NSA.

10. Prior to that, I was the Technical Director of the Analytical Services Office. In such position, I was responsible for handling all technical issues relating to the acquisition, development and distribution of signals intelligence for the agency's 6,000 analysts. These analysts were responsible for analysis and reporting for the entire world.

11. My duties included working with foreign governments who receive signals intelligence collected by the NSA. These include the so-called "Five Eyes" – *i.e.* the intelligence agencies for Australia, Canada, New Zealand, and the United Kingdom, in addition to the United States.

12. At the NSA, I was the primary designer and developer of a number of programs designed to acquire and analyze very large amounts of information and data files. The final program I was addressing dealt with the acquisition of information from the internet.

Opinions

13. WikiLeaks did not receive the stolen data from the Russian government.

14. Intrinsic metadata in the publicly available files on WikiLeaks demonstrates that the files that were acquired by WikiLeaks were delivered in a medium such as a thumbdrive.

physically local to the DNC.

Supporting Reasoning

16. Forensic Fingerprint - An anomaly of the DNC data on the WikiLeaks site is that all last modified date and time stamps end in an even number. This is a side effect of files that have been copied directly from a source system (such as a server) to a physical medium such as a thumbdrive. This is in contrast to files that have been copied from one server over the internet to another system as used by hackers (*i.e.* Linux).

17. Time signatures – Guccifer 2.0 posted (time stamped) files it reveals a time signature that allows us to calculate the speed the files was copied. As each file is copied from the source to the destination, the file is time stamped. All of the files constantly demonstrate they were copied at speeds massively greater than internet speeds. This data came from "Guccifer 2.0." Again, consistent with files copied directly and manually to a thumbdrive inside the building.

18. Missing day – The DNC files from WikiLeaks reveal that they were copied in three tranches, on May 23, 25, and 26; skipping the 24th. This would be more consistent with files that were being covertly copied when opportunities presented themselves, as opposed to a collection of files that had already been gathered and then transmitted as a collection to a destination such as WikiLeaks.

19. Time zone - While a weak indicator, it needs to be noted that the time zones of the files are more consistent with working hours in America rather than other sides of the globe.

I declare under penalty of perjury that the foregoing is true and correct. Executed in _______this _9th___ day of May, 2019.

William E. Binney

Exhibit 1

Internal Exhibit C

Peter Clay CISSP

cpthuah36@gmail.com · www.linkedin.com/in/peclay · m: 703-220-3531

Professional summary

Leader, advisor, mentor, strategist and experienced executive in the field of information security with a proven record of building security programs or consultancies and executing either on a global scale. Passionate about the role of security as both a protective and enabling function within the enterprise and skilled at delivering market beating results and capabilities. Experienced leading an internal CISO function, an external consultancy or participating in the development of new security tools and methodologies as a single practitioner.

Internationally experienced cyber security executive and senior advisor with 23 years of service to the world's largest private and public-sector entities, Fortune 1000's, small to mid-sized organizations, US legislative and executive branches, and regulatory agencies.

Summary of skills

- Leadership - startups to large multinationals
- M&A due diligence and integration
- Enterprise security design and architecture
- Managed Security Services Provider (MSSP)
- Network Intrusion Detection Systems (NIDS/NIPS)
- Host Intrusion Prevention Systems (HIDS/HIPS)
- Network Security Monitoring (NSM)
- Security Operations Centers (SOC)
- Event Correlation and Log Aggregation (SEM)
- Integrated security monitoring solutions (SEIM)
- Network and host forensic analysis
- Anti-virus/malware enterprise solutions
- Computer incident response (CIRT/CSIRT)
- Business Continuity/Disaster Recovery (BC/DR)
- Policy development and enforcement
- Enterprise vulnerability assessment systems
- PKI/digital rights management solutions
- Security Intelligence Fusion Centers
- Strategy and management consulting
- Security Analytics and Operations
- System development lifecycle
- Regulatory compliance (FISMA, SOX, DFAR, PCI)
- Privacy compliance (Privacy Act, GDPR)
- IT Governance (NIST, DOD, CobIT, ITIL)
- Cross functional collaboration
- Intellectual property control methods
- Security evangelism/client engagement
- Technology project management
- Executive briefings and presentations
- Security strategies and roadmaps
- Training development and delivery
- Venture integration/M&A analysis
- Enterprise risk management

Career summary

COO	Dark3	2019-Present
Owner	Fenris	2002 – present
Partner	Small Federal Consultancy	2016 – 2018
CISO	Qlik	2015 –2016
CISO	Invotas	2014 – 2015
Director II/CISO Fed Practice	Deloitte	2010 – 2014
Senior Manager	Deloitte & Touché LLP	2005 – 2010
Senior Manager	Urbach, Hacker, Young	2002 – 2004
Partner	CoDevelop	1995 – 2002

Certifications and Education

- Hendrix College (1985)
- Oxford University (1983)
- Certified Information Systems Security Professional (CISSP)
- Top Secret DoD Clearance
- Bachelor of Arts
- Junior Year Abroad Program
- Member, ISC^2

🟦 - consulting 🟩 - employment

Professional experience

Fenris, *Charlottesville, VA* 2002 – present

Founder

Strategic advisor and independent expert in the fields of cyber security, managed services, regulatory compliance, and virtual CISO services. Specialized in supporting small to mid-sized enterprises (SME) implement, design, manage and operate their information security programs efficiently and effectively while meeting their compliance and reporting obligations.

Automated Financial Systems *New York, NY* 2002-2010

Managed Security Services

Retained to develop and deliver a complete managed security solution to the pioneer in online stock and commodities trading. Services included network/host intrusion detection, firewall management, incident response, PKI design, vulnerability management, security architecture and compliance reporting (NYSE/AMEX exchange requirements). Resulted in compliant security operations and identified as a key factor in winning bids on over $15 mm in new business.

Potlatch Timber Products *Warren, AR* 2004

Lead Security Architect, Industrial Controls

Developed and delivered secured industrial control solution that enabled remote vendor support via modem to 16 machine centers located in Central Arkansas. Identified as reducing major machine center downtime by over 74% and contributed to increasing over all mill throughput by 7% year over year.

Katzcy *Reston, VA* 2018

Virtual CISO

Retained to develop and implement company and product strategy for Katzcy's compliance with NIST 171 requirements in support of their Department of Defense contractor support. Designing the technology stack, completing the risk assessment, security plan and disaster recovery documentation while performing the continuous monitoring function and documenting the results.

ZTP *Rosslyn, VA* Sep 2016 – June 2018

Partner

Joined the partnership to develop the federal practice business pipeline, develop unique offerings for the federal and commercial markets and mentor the in-house security talent and identify additional talent that could add value to our operations. In 18 months with ZTP led the capture of over $70M in new federal business and helped the company expand into 3 new federal clients. Additionally, led the development of a commercial small to mid-sized business focused managed security practice that was recently selected by a global insurance company to be their exclusive go to market partner for a global launch by pairing their small business insurance products with ZenOpz managed technology stack.

ZTP Client engagements:

Small Business Administration *Washington, DC* Sep 2016-June 2018

Managed Security Services

Retained to develop and deliver complete security program support to the entire agency to include build a Security Operations Center from scratch, support over 30 authorization and accreditation packages annually, provide all security engineering, provide security intelligence functions and processes, be the key resource for disaster recovery and business continuity operations, perform all vulnerability management functions, provide key support for patch management, provide user training for over 6000 employees and enterprise wide penetration testing. During my tenure the scale of the program more than doubled and revenue jumped from $3.5mm to over $10 mm per annum.

General Services Administration, *Washington DC* Sep 2016-June 2018

Subject Matter Expert

Supported the accreditation and testing processes of ten vendors on a government wide contract to provide internet and networking services across the federal government. Developed a streamlined approach to performing the testing processes necessary for the accreditation and worked with the government selected vendors to prepare their documentation for submission and testing. Results of the streamlined testing efforts resulted in a follow-on award of over $2mm for FY 2019 to continue program support.

ZTP Commercial *Charlottesville, VA* Sep 2016-June 2018

Founder/Lead Architect

Developed a small business focused outsourced security program offering based on open source/free software designed to provide small to mid-sized organizations with the ability to execute a full security program in support of their specific compliance and data protection requirements. Developed and documented the 360-review process which married Risk Assessment, Security Maturity Model, Threat Matrix and Vulnerability assessments to provide a holistic view of the client's information security posture. Designed and built the tech stack supporting the process to make maximum use of automation/orchestration to reduce the headcount required to provide the operational support. Was selected over 3 national vendors as a go to market partner with a national education tech company with 1400 clients in the US and selected by an international insurance vendor as the launch partner for a global re-launch of their cybersecurity insurance product lines.

Qlik, *Philadelphia, PA* May 2015-Sep 2016

Chief Information Security Officer

As the first CISO hired by Qlik and the senior security practitioner on staff, I implemented the initial information security program at Qlik by rapidly creating cyber and data protection capabilities using limited staff and very limited financial resources. At the end of the first year the Qlik security program was protecting the primary assets of a software company operating in 32 countries globally.

- Stood up a combined operations/security Global Operations Center to provide a consolidated monitoring/triage function for the global network to include building 28 playbooks to support entity requirements in the first 6 months of operation
- Implemented entity wide security policies and procedures
- Managed 2 cycles of SOX 404 review successfully mitigating multiple findings from previous reviews
- Supported the re-architecting of the Salesforce solution to include minimal required security controls
- Supported federal sales by leveraging relationships and experience to manage federal security requirements for cloud and on prem solutions
- Implemented the first vulnerability management program in corporate history
- Designed, developed and led the CSIRT capability for the company
- Developed and supported the re-architecting of the global network to increase security of critical assets and reduce bottlenecks and single points of failure across the globe
- Created and evangelized a cyber governance model to leveraging open source tools and capabilities to rapidly increase the security maturity of the program
- Maintained active private/public engagement with US and international law enforcement, intelligence, national security, and industry partners in support of issues and requirements

Invotas, *Alexandria VA* May 2014 – May 2015

CISO, Consulting Lead

As the client facing cyber security leader for Invotas my duties included securing our cloud-based/on premise orchestration engine, documenting our security environment, interfacing with clients regarding our risk management practices for the commercial and classified efforts and managing the development of the consulting and sales engineering group. Additionally, I was designated one of the thought leaders and authors for the company and worked with the marketing group to deliver timely articles and thought pieces to industry publications, manage interviews with national press and speak on a variety of topics at international security programs in the US, UK and UAE.

- Primary input into the development and operational requirements for the software products
- Responsible for developing the standardized "playbooks" for client use to include: endpoint, network and application incident response, automation supporting security intelligence enrichment functions, automated reporting and analysis capabilities, secure environment maintenance and integration with multiple classes of tools to include SEM, SIEM, Firewall, Router, HID, NID, Intelligence applications, endpoints and applications
- Delivered over 40 in person presentations ranging from keynote at a regional conference to small groups internationally (US, Europe, Middle East)
- Developed and evangelized original end-to-end company security strategy to integrate enterprise, product, and customer security objectives as a continuous cyber maturity model
- Architected and led global cyber governance and standardization efforts to align processes with applicable NIST, DOD and ISO requirements
- Led a multinational team of cyber security professionals and delivered security and sales engineering services globally
- Created and evangelized a cyber governance model to leverage automation and orchestration investment in cyber security initiatives for our clients
- Active private/public engagement with US and international law enforcement, intelligence, national security, and industry partners to enhance orchestration awareness, capabilities, and training to US intelligence entities

Deloitte LLP, *Rosslyn, VA* Feb 2010 – May 2014

Chief Information Security Officer Deloitte Federal Practice

Developed and implemented a separate federally compliant computing environment that enabled the 8000 federal practitioners to operate without changing their hardware or computing environments. In addition, the Federal CISO team developed a federal cloud offering that provided the federal practice with the ability to leverage federally compliant infrastructure, platform and applications as a service and include those offerings to federal clients. The success of the federal program resulted in the transfer of the Federal Practice CISO team to the US Firms Information Risk and Compliance Group where I was rapidly promoted from Senior Manager to Director II and took on additional responsibilities to include firm wide security architecture and leadership of IRC.

- Reduced compliance efforts and requirements managed by the US firm from over 300 to 2 (FISMA/Firm global requirements)
- Responsible for securing ~60,000 personnel (on 4 continents) and 35% share of Deloitte's global $28B and 210,000- employee enterprise environment
- Restructured and led M&A Cyber Due Diligence and Remediation Program to enable accelerated integration of 19 acquired environments through risk-based assessment and remediation model
- Architected and oversaw deployment of a $12M global enterprise SIEM solution
- Architected and oversaw deployment of a $2M global Data Loss Prevention Solution
- Established US Firm's PKI infrastructure and deployed it to over 18 countries in 8 months
- Provided strategic guidance in development, deployment and use of a custom internally-developed SEM/DLP/Backup solution designed for real-time forensic analysis and incident response support
- Responded to every major intrusion incident on Deloitte's networks worldwide from 2010-2014
- Architected and deployed a FEDRAMP certified solution in support of Deloitte's federal practice that included Infrastructure, Platform and Application components in 4 months
- Oversaw PCI-DSS implementation for an 800-room hotel/training center
- Active private/public engagement with US and international law enforcement, intelligence, national security, and industry partners to enhance threat intelligence awareness, defensive capabilities, and maturity benchmarking of the firm's cyber efforts as part of a long-term continuous improvement plan
- Developed & delivered award winning security training programs to train over 60,000 users annually using computer-based training, phishing exercises, customized training and executive briefing series on cybersecurity
- Rated in the top 10% of my peers throughout my tenure at Deloitte LLP

- Directly involved with over 80 interactions with F100 customers, partners, Federal and State CISO/CIO/CEO level

Deloitte & Touché LLP, *Rosslyn, VA* Aug 2005 – Feb 2010

Senior Manager

Hired as the 16th member of the Deloitte & Touché LLP Enterprise Risk practice and over the course of 4.5 years was integral to the capture of $65M in revenue at 6 different executive agencies, developed multiple federally focused processes (penetration testing, continuous compliance, risk management) still in use today and was part of the leadership team that delivered 400% growth over my tenure. Additionally, developed relationships with multiple software vendors to increase federal and commercial opportunities. Consistently rated in the top 25% of my peers in annual reviews.

Deloitte & Touch LLP Client Engagements:

Department of Homeland Security (DHS), *Crystal City, VA* 2008–2010

Senior Enterprise Risk Team Lead

- Designed and implemented the reference and solution architecture for the initial cloud environment to facilitate intelligence sharing between multiple agencies
- Supported the design and implementation of security processes for 8 agency wide applications
- Oversaw the authorization and accreditation process for multiple federal environments through a team of ISSO's
- Participated in developing formal feedback for DHS response to NIST regarding Special Publication 800-53
- Participated in developing the DHS policy regarding the accreditation of third party applications

World Bank, *Washington, DC* 2009

Penetration Test Lead

- Performed a series of penetration tests versus World Bank environments
- Developed the executive report deliverables and presented them to client leadership
- Architected the ongoing testing program on behalf of World Bank

Department of Defense, *Washington, DC* 2006-2008

IT Audit Lead

- Led multiple IT audits of general computer controls and technical configurations on behalf of DoD Inspector General with a team composed of Deloitte and contractor personnel
- Performed analysis of technical configurations and architectures throughout DoD in accordance with DoD instructions
- Developed recommendations for architecture, configuration and operational improvements
- Primary author of 4 DoD IG reports on various DoD applications

United States Mint, *Washington, DC* 2006-2007

IT Audit Lead

- Led the initial reviews performed in accordance with OMB A-123 (SOX for the federal government)
- Reviewed 6 Mint locations simultaneously with multiple teams of auditors and information security professionals
- Completed the time compressed project in 75% of the allotted time resulting in a government savings of over $1.2M in the first year
- Examined 30+ mission-critical business applications and functional components
- Audited critical infrastructure services: SIEM, Endpoint, Logging, Incident Response
- Determined compliance state at component, application, and functional levels

Urbach, Hacker, Young LLC *Washington, DC*

Senior Manager

Hired as the deputy leader of the IT Audit and Security team to provide leadership to multiple Navy Inspector General Audits and develop methodologies to support the growth of the IT security practice. Doubled the size of the practice in two years and created three new lines of business to support penetration of the commercial and federal markets.

UHY LLP Client Engagements:

Navy IG, *Washington DC* 2002-2004

Team Lead

- Led multiple reviews of Navy applications spanning global operations to include payroll, logistics, training and infrastructure systems
  - Deployed teams globally to perform local testing processes
  - Completed 100% of reviews on time and on budget
  - Examined 10+ applications and processes by determining compliance state at component, application and functional levels
  - Performed initial penetration testing in support of Navy IG Audits

New York Counties, *New York* 2002

Team Lead

- Led HIPAA reviews for hospitals in 9 New York counties
- Completed 100% of reviews on time and on budget
- Developed a data discovery and analysis technique that created significant operational efficiencies
- Used the operational efficiencies to expand the scope to include additional testing services in support of hospital disaster recovery plans

Deutsche Bank, *Global* 2004

Security Engineer/Architect

- Planned, architected and trained 6 travel teams on the Securify application for deployment throughout Deutsche Bank's global environment
- Managed all aspects of 6 simultaneous implementations every week for 5 weeks for a total of 30 installations on 6 continents
- Developed the formal documentation and "playbook" for deploying the Securify application along with the initial

CoDevelop, *Charlottesville, VA* 1995 – 2002

Partner

General Partner in CoDevelop an internet incubator located designed to identify very early stage companies and provide them with the resources necessary to realize the value of their concepts. Developed the 5-50-500 strategy which allowed companies to rapidly develop from a "back of the napkin" stage to effective market entry and a candidate for institutional investment. Provided operational leadership and mentorship to the early stage companies and successfully helped 4 of the companies to exit the program

Exhibit 1

Internal Exhibit D

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA

v.

No. 19-cr-18 (ABJ)

ROGER J. STONE, JR.

Defendant.

______________________________________/

DECLARATION OF PETER CLAY

I am Peter Clay and I hereby declare:

Background

1. I am an internationally experienced cyber security executive and senior advisor with 23 years of service to the world's largest private and public-sector entities, small to mid-sized organizations, US legislative and executive branches, and regulatory agencies.

2. Over my career I have worked with and for International Banks, State and Local Governments, the U.S. Navy, U.S. Mint, Department of Defense, Department of Homeland Security, General Services Administration, and Small Business Administration.

3. A true and correct copy of my *curriculum vitae* is attached as an Exhibit.

4. The below expresses my opinions and my reasoning is set out after the opinions. The reasoning is based upon publicly available documents from WikiLeaks.

Opinions

5. Given the information that is available it is more likely that the data posted to Wikileaks was removed by someone with physical access to the computing equipment rather than removal by an external actor.

6. Intrinsic metadata in the publicly available files on WikiLeaks demonstrates that the files that were acquired by WikiLeaks were most likely delivered in a medium such as a thumbdrive.

7. The data indicates that the files were likely acquired from the DNC manually and physically local to the DNC.

Supporting Reasoning

8. Forensic Fingerprint - An anomaly of the DNC data on the WikiLeaks site is that all last modified date and time stamps end in an even number. This is a side effect of files that have been copied directly from a source system (such as a server) to a physical medium such as a thumbdrive. This is in contrast to files that have been copied from one server over the internet to another system as used by hackers (*i.e.* Linux).

9. Time signatures – On the Guccifer 2.0 posted (time stamped) files it reveals a time signature that allows us to calculate the speed the files was copied. As each file is copied from the source to the destination, the file is time stamped. All of the files constantly demonstrate they were copied at speeds significantly greater than internet speeds. This data came from "Guccifer 2.0." Again, consistent with files copied directly and manually to a thumbdrive inside the building.

10. Missing day – The DNC files from WikiLeaks reveal that they were copied in three tranches, on May 23, 25, and 26; skipping the 24th. This would be more consistent with files that were being covertly copied when opportunities presented themselves, as opposed to a collection of files that had already been gathered and then transmitted as a collection to a destination such as WikiLeaks.

11. Time zone - While a weak indicator, it needs to be noted that the time zones of the files are more consistent with working hours in America rather than other sides of the globe.

12. From the information that has been provided it appears likely that standard forensic techniques regarding the preservation of the hard drives and volatile memory were not followed which leaves only the review of publicly available information as the forensic source.

I declare under penalty of perjury that the foregoing is true and correct. Executed in _______this _9th___ day of May, 2019.

Peter Clay

Peter Clay